



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.  | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.        | CONFIRMATION NO. |
|--|-------------|----------------------|----------------------------|------------------|
| 10/040,436   | 01/09/2002  | Hideaki Watanabe     | SON-2321                   | 4774             |
| 23353  | 7590        | 09/28/2005           |                            |                  |
| RADER FISHMAN & GRAUER PLLC<br>LION BUILDING<br>1233 20TH STREET N.W., SUITE 501<br>WASHINGTON, DC 20036 |             |                      | EXAMINER<br>ELMORE, JOHN E |                  |
|  |             |                      | ART UNIT<br>2134           | PAPER NUMBER     |

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/040,436

Applicant(s)

WATANABE ET AL.

Examiner

John Elmore

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 and 17 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 and 17 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 January 2003 is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

### DETAILED ACTION

1. In response to the previous office action, Applicant has amended claim 6 and has cancelled claims 13-16. Claims 1-12 and 17 have been examined.

#### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. **Claims 1, 2, 6, 8 and 12-17 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Shear et al. (US 6,157,721), hereafter Shear, in view of Whittle ("Public Key Authentication Framework: A Tutorial," whitepaper, First Principles Consulting, June 1996).

**Regarding claim 1**, Shear discloses a public key certificate issuing system comprising:

a certificate authority for issuing a public key certificate of an entity which uses said public key certificate (verifying authority) and said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, transferring a public key certificate between said plurality of certificate authorities response to said public key certificate issuing request, attaching a digital signature on message data constituting said public key certificate in accordance with

said different signature algorithm at each certificate authority, and issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms (Fig. 7; col. 10, lines 32-59; col. 14, line 61, through col. 8, line 22; col. 16, lines 12-36).

But Shear does not explain that the system comprises a registration authority for sending a public key from an entity under certificate issuing request received control to said certificate authority.

However, Whittle teaches a public key authentication system comprising a registration authority for sending a public key from an entity under certificate issuing request received control to a certificate authority for the purpose of administrative efficiency by acting as a conduit between the certification authority and an entity requesting certification (organizational registration authority sends a request for issuance to organizational certification authority; page 8).

Therefore, it would be obvious to one of ordinary skill in the computer art at the time the invention was made to modify the invention of Shear with the teaching of Whittle to provide a system comprising a registration authority for sending a public key from an entity under certificate issuing request received control to said certificate authority. One would be motivated to do so in order to increase administrative efficiency in the handling of certification requests.

**Regarding claim 2**, the modified device of Shear and Whittle is relied upon as applied to claim 1, and Shear and Whittle further teach that said plurality of certificate authorities include a Rivest-shamir-Adleman certificate authority for executing signature

generation processing based on a Rivest-shamir-Adleman signature algorithm and an elliptic curve cryptography certificate authority for executing signature generation processing based on an elliptic curve cryptography algorithm, said signatures stored in said multi-signed public key certificate including a signature based on said Rivest-Shamir-Adleman signature algorithm and a signature based on said elliptic curve cryptography signature algorithm (Shear, col. 13, lines 43-49). Therefore, for reasons given above, such a claim also would have been obvious.

**Regarding claims 6 and 8**, this is a method version of the claimed system discussed above (claims 1 and 2), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

**Regarding claim 7**, the modified device of Shear and Whittle is relied upon as applied to claim 6, and Shear and Whittle further teach that at least one of said plurality of certificate authorities executes a step of generating a signature for a signed public key certificate by applying a signature algorithm which is signed public key different from that attached to said certificate and attaching the generated signature to said signed public key certificate (different algorithms used by subsequent signers to defeat cryptographic attack; col. 16, lines 22-36). Therefore, such a claim also would have been obvious.

**Regarding claim 12**, this is an information-processing-apparatus version of the claimed system discussed above (claim 1). Thus, for the reasons provided above, such a claim also would have been obvious.

**Regarding claim 17**, this is a program-storage-medium version of the claimed system discussed above (claim 1). Thus, for the reasons provided above, such a claim also would have been obvious.

2. **Claims 3 and 9 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Shear and Whittle, as applied to claim 1, and further in view of Chokhani ("Comment on RFC 2527," The Internet Society, March 1999).

**Regarding claim 3**, Shear and Whittle do not explicitly explain that at least one of said plurality of certificate authorities has a configuration for executing processing of storing a generated signature and signature information including signature algorithm information associated with said generated signature into an extended area of said public key certificate.

However, Chokhani teaches a public key system wherein at least one of said plurality of certificate authorities has a configuration for executing processing of storing certificate policies into an extended area of said public key certificate for the purpose of providing storage of additional certificate policies that are not provided for in the basic X.509 certificate policy framework, particularly where the policies are highly customized (e.g. certificate policies extension, section 3.3.1, and policy mappings extension, section 3.3.2; pages 5-7).

Therefore, it would be obvious to one of ordinary skill in the computer art at the time the invention was made to modify the modified device of Shear and Whittle with the teaching of Chokhani such that at least one of said plurality of certificate authorities has

a configuration for executing processing of storing a generated signature and signature information including signature algorithm information associated with said generated signature into an extended area of said public key certificate. One would be motivated to do so because the basic certificate framework is insufficient to store policy information regarding multiple signatures using different signature algorithms, particularly where the policies are highly customized.

**Regarding claim 9**, this is a method version of the claimed system discussed above (claim 3), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also would have been obvious.

3. **Claims 4 and 10 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Shear, Whittle and Chokhani, as applied to claim 3, and further in view of Levi et al. ("A Multiple Signature Based Certificate Verification Scheme," Proceedings of BAS'98, The Third Symposium on Computer Networks, June 1998), hereafter Levi.

**Regarding claim 4**, the modified device of Shear, Whittle and Chokhani as applied to claim 3 is relied upon for teaching the storing of signature information including signature algorithm information associated with the generated signature into an extended area.

But Shear, Whittle and Chokhani do not explicitly explain that at least one of said plurality of certificate authorities has a configuration for executing processing of storing a generated signature into an area other than a basic area and an extended area of said public key certificate.

However, Levi teaches a public key certification system wherein at least one of a plurality of certificate authorities has a configuration for executing processing of storing a generated signature into an area other than a basic area and an extended area of a public key certificate for the purpose of accommodating multiple signatures, particularly where the existing frameworks such as X.509 do not provide for them (append multiple signatures to the end of the certificate; see section 6.2).

Therefore, it would be obvious to one of ordinary skill in the computer art at the time the invention was made to modify the modified device of Shear, Whittle and Chokhani with the teaching of Levi such that at least one of said plurality of certificate authorities has a configuration for executing processing of storing a generated signature into an area other than a basic area and an extended area of said public key certificate. One would be motivated to do so in order to accommodate multiple signatures, particularly where the existing frameworks such as X.509 do not provide for them.

**Regarding claim 10**, this is a method version of the claimed system discussed above (claim 4), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also would have been obvious.

4. **Claims 5 and 11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Shear and Whittle, as applied to claim 1, and further in view of Levi.

**Regarding claim 5**, Shear and Whittle do not explicitly explain that at least one of said plurality of certificate authorities has a configuration for executing processing of



storing, into said public key certificate, flag information indicating whether at least two signatures are included in said public key certificate.

However, Levi teaches that the existing X.509 standard for assumes a single signature and that the structure would need to be modified for the purpose of accommodating multiple signatures (section 6.2). And the Examiner takes official notice that one of ordinary skill in the computer art at the time the invention was made would recognize the storing of flag information as a common technique in distinguishing between one of two different states, in this case the state indicating at least two signatures are included in a public key certificate or the state indicating a single signature.

Therefore, for the reasons given above, such a claim also would have been obvious.

**Regarding claim 11**, this is a method version of the claimed system discussed above (claim 5), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also would have been obvious.

### ***Response to Amendment***

2. Applicant's arguments filed 7 July 2005 have been fully considered but they are not persuasive.

Regarding Applicant's argument that Shear "fails to disclose, teach, or suggest at least issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms" (Remarks, pages 7 and 8), it is helpful to note that in

the specification Applicant defines a multi-signed public key certificate as “a public key certificate having two or more digital signatures generated on the basis of different signature generating algorithms” (Applicant, page 43). Shear teaches that “multiple digital signatures... can be created for the same load module” (col. 14, lines 61-63) for the purpose of certifying the load module with a public key certificate (col. 10, lines 32-59). Shear also teaches that “different digital signatures can also be made using... different encryption algorithms” (col. 15, lines 14-16). Hence, one of ordinary skill in the art would recognize that the multiple signatures created for the same load module are part of a single public key certificate used to authenticate that module. The fact that the digital signatures are “different” does not suggest that they constitute wholly different certificates; rather, it merely supports the fact that each signature uses a different signature algorithm so that the single, signed certificate is made more secure.

Regarding Applicant’s argument that it is inappropriate to combine Whittle with Shear because Whittle “fails to disclose, teach, or suggest at least issuing a multi-signed public key certificate” (Remarks, page 8), it is noted that Whittle does not teach a multi-signed public key certificate. However, the number of signatures attached to a public key certificate, whether one or many, is not relevant to the application of Whittle’s teaching to Shear. Shear teaches that multiple certificate authorities are employed in constructing a public key certificate, each certificate authority providing a digital signature to the multi-signed certificate (col. 10, lines 32-44). Whittle teaches a registration authority for sending a public key from an entity to a certificate authority (Whittle, page 8). As such, one of ordinary skill in the art would recognize that Whittle is

applicable to Shear for every instance where a digital signature is procured. That is, the use of a registration authority as an intermediary to a certificate authority is substantively the same for the modified system of Shear and Whittle employing multiple digital certificates (and therefore multiple certificate authorities) as it is for the construction of a public key certificate containing only a single digital certificate.

### ***Conclusion***

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

John Elmore



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100